Comentarios al Decreto de Ciberseguridad del MinTic

Índice

1. Comentarios Generales

1.1. Es necesario que el diseño de las políticas nacionales de seguridad digital se construyan a partir de procesos incluyentes y transparentes

Si bien el decreto de ciberseguridad actualmente se encuentra en periodo de comentarios públicos que incluyen a la sociedad civil, es necesario señalar que en general el proceso de implementación del Conpes 3995 de 2020, del que se desprende esta regulación, no ha incluido a la sociedad civil durante su implementación. Esta es una deuda que no se salda con 18 días de plazo para comentarios públicos.

Aunque entendemos que el primer paso para la creación de la norma requiere acuerdos intergubernamentales, consideramos que pudo hacerse un esfuerzo para incorporar las visiones de múltiples partes interesadas en este tema antes de socializar públicamente, eso no sucedió. Como bien queda constancia en el Formato de Memoria Justificativa, anexo al borrador de decreto, la única entidad no gubernamental que tuvo un papel importante en la formulación de la norma actual fue la Organización de los Estados Americanos (OEA), participación respecto de la cuál no se ha hecho pública ninguna información.

En igual sentido, si bien se menciona, que respecto del Modelo de Gobernanza de Seguridad Digital se "se contó con aportes obtenidos en espacios de trabajo en los que aportaron las diferentes partes interesadas en Seguridad Digital en Colombia", según información enviada por el MinDefensa, en respuesta a un derecho de petición de Fundación Karisma, estas entidades se limitan a organismos adscritos al propio ministerio y no incluyen ni entidades estatales relacionadas con derechos humanos ni, de nuevo, a la sociedad civil.

Siendo así, la participación de múltiples partes interesadas (academia o intermediarios de internet), y especialmente la ciudadana en la formulación de la actual política de gobernanza en seguridad digital es pobre y este problema se evidencia de forma clara en el enfoque del decreto objeto de comentarios. En este sentido, este ejercicio público de comentarios es la primera iteración abierta y pública pero no debería ser la final.

Sugerimos que los responsables de desarrollar esta regulación tomen como insumo de análisis la "Guía para realizar la consulta pública en el proceso de producción normativa"[1] publicada por el gobierno colombiano en 2017 y las sugerencias de los documentos de la OCDE como el de "Recomendaciones del Consejo sobre la gestión de riesgos de seguridad digital para la prosperidad económica y social" (2015). En este último se advierte que las políticas en este tema deberían "ser el resultado de un enfoque intergubernamental coordinado y de un proceso abierto y transparente en el que participen todas las partes interesada"[2].

Es indispensable que se abran espacios para que la ciudadanía participe del modelo de gobernanza de ciberseguridad y que el enfoque general de la norma prevea que la ciudadanía, y no el propio Estado, sea su principal beneficiario, pues, dada la acelerada

[1] https://colaboracion.dnp.gov.co/CDT/Mejora%20Regulatoria/Documentos/Gu%C3%ADa_consulta_p%C3%BAblica.pdf

[2] OECD. Legal Instruments. Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity. Disponible en: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0415

transformación digital de nuestra sociedad, ya no hay duda de la importancia de la seguridad digital para todos los espacios de la vida social y económica de un país.

Finalmente, en términos de la elaboración de este documento quisiéramos recordar la influencia de la OCDE en estos temas. Debemos recordar que la voluntad del gobierno de ingresar a la OCDE hizo que en 2015-2016 la versión final del Conpes de seguridad digital fuera ajustado de manera sustancial para cumplir con los lineamientos de este organismo internacional[3]. Aunque entrar al club es una presión que ya no tenemos, sin embargo resulta necesario indicar que siendo miembros de ese organismo internacional y habiendo adoptado sus lineamientos en la materia, el texto actual está lejos de adoptarlos.

Consideramos que en el marco de nuestra Constitución el diseño de esta política debe tener importante conexión con el respeto de los derechos humanos y debería incorporar una importante apuesta por aplicarlos, existe ya mucha literatura que soporta este propósito. Sin embargo, el poco tiempo que se ha dado para comentar este complejo borrador de decreto no permite que hagamos muchas recomendaciones en este campo. Con el antecedente de 2016, el error de no tener en cuenta los lineamientos de la OCDE desde la fase inicial de la formulación de la política pública, sabemos que en la práctica que el borrador de Decreto está tan alejado de los lineamientos de la OCDE es lo que obligará a hacer cambios sustanciales. Así decidimos concentrar los esfuerzos en mostrar lo alejado que esta política está de los estándares OCDE y resaltar la forma como en tales estándares se reconoce la conexión de la seguridad digital con los derechos humanos, algo que el borrador de decreto solo sugiere.

Recomendación:

- Aplicar la “Guía para realizar la consulta pública en el proceso de producción normativa” del gobierno colombiano para garantizar una debida participación en el proceso de elaboración de esta política pública.
- Analizar y aplicar los lineamientos OCDE en materia de seguridad digital que incluyen los siguientes documentos[4]:
  - OECD. Legal Instruments. Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity. Consideren también el documento que las acompaña[5].
  - OECD, Legal Instruments. Recommendation of the Council on the Protection of Critical Information Infrastructures[6]
  - OECD, Going digital toolkit, policy note. Enhancing the digital security of critical activities[7].
  - OECD, Políticas de banda ancha para América Latina y el Caribe[8]
  - Los informes OECD sobre seguridad digital de los productos y los de

[3] https://web.karisma.org.co/que-es-el-conpes-de-seguridad-digital-y-por-que-esta-mal/ y https://web.karisma.org.co/comentarios-al-borrador-de-conpes-de-seguridad-digital/

[4] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0415 (publicación que incluye el documento que acompaña las recomendaciones https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf)

[5] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0415 (puede consultarse también la publicación que incluye el documento que acompaña las recomendaciones https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf)

[6] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0361

[7] https://goingdigital.oecd.org/data/notes/No17_ToolkitNote_DigitalSecurity.pdf

[8] https://www.oecd-ilibrary.org/science-and-technology/politicas-de-banda-ancha-para-america-latina-y-el-caribe_9789264259027-es

manejo de vulnerabilidades[9]. ○ OECD, Guidelines for Cryptography Policy[10]

1.2. La política nacional de seguridad digital en Colombia debe poner en el centro a las personas y reconocer su deber de proteger sus derechos.

Los importantes beneficios de la digitalización y la transformación digital de nuestras sociedades expone a todas las personas a un riesgo de seguridad digital que conlleva pérdidas financieras, perturbaciones o interrupciones de las actividades, robo de la propiedad intelectual, daños a la reputación y violaciones de la privacidad, pérdidas de competitividad, amenazas a la libertad de expresión, así como daños físicos y medioambientales.

La referencia a este tipo de amenazas es cada vez más frecuente, así en el Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión (2015)[11], David Kaye, se abordaron cuestiones claves de la seguridad digital -el cifrado y el anonimato en las comunicaciones digitales. Estas protecciones no sólo son importantes para grandes industrias como los medios de comunicación -fuertemente conectados con la libertad de expresión- en lo que respecta a su misión, sino también para la democracia en general.

En general todas las publicaciones OCDE son claras en que se debe priorizar a las personas en materia de seguridad digital, en concreto las Recomendaciones sobre la gestión del riesgo digital[12] establece cuatro principios: el primero, es impulsar que los Estados trabajen para mejorar concienciación, competencias y capacitación de las personas; el segundo, desarrollar la co-responsabilidad -principio que tenemos en el Conpes de seguridad digital sin mucho desarrollo-; en tercer lugar, indica que los derechos humanos deben ser objetivo central y, finalmente, se indica que se debe trabajar por la cooperación con las múltiples partes interesadas en estos temas, es decir con todo el gobierno, con el sector privado, con la academia, con la sociedad civil, etcétera.

Los documentos de la OCDE relacionados con seguridad digital en general no solo hacen referencia genérica a los derechos humanos reconocen frecuentemente el impacto en privacidad usualmente y algunos, como el de la protección de los denunciantes o informantes para luchar contra la corrupción, también apoyan la idea de la responsabilidad de los gobiernos para garantizar la libertad de las personas. En ese caso para hablar contra la corrupción económica y política fuerte.

De hecho, un texto como el del decreto termina ignorando los más recientes documentos de la OCDE que buscan fomentar la gestión de vulnerabilidades donde se reconoce el papel de los investigadores de seguridad en la seguridad digital. Atender estos lineamientos debería llevar a una política nacional a evaluar y actuar frente a la falta de protección hacia su importante actividad.

---

[9] Consultar la página del grupo de trabajo en seguridad digital de la OCDE https://www.oecd.org/digital/ieconomy/digital-security/

[10] https://www.oecd.org/sti/ieconomy/cryptography.htm

[11] https://www.ohchr.org/en/issues/freedomopinion/pages/callforsubmission.aspx

[12] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0415

Es en este tipo de políticas que se debe desincentivar y condenar que los propietarios y responsables de sistemas o servicios en donde se encuentren vulnerabilidades -incluso actores estatales-, usen herramientas legales para amenazarlos con acciones judiciales en lugar de acoger sus informes de vulnerabilidad. El trabajo de la OCDE sobre el tratamiento de las vulnerabilidades ha identificado que las principales áreas de riesgo legal para los investigadores incluyen el derecho penal, el derecho de propiedad intelectual, el derecho de protección de datos y el derecho contractual. Este es un campo en el que, la política que contempla el decreto de ciberseguridad tal como está diseñada guarda absoluto silencio al punto que no hay estrategias para mejorar el conocimiento sobre el papel clave de los investigadores de seguridad en la mejora de la respuesta de la seguridad digital y proveerles canales de confianza para hacer sus reportes.

Es muy claro el vínculo de la seguridad digital con los derechos especialmente a la libertad de expresión y la privacidad, pero cada vez es más evidente que también se vincula con otros como la salud, el medio ambiente, etcétera. Además, es reconocido en todos los documentos de la OCDE sobre el tema, y se afirma que su protección debe ser considerada en los planes nacionales de seguridad digital.

Actualmente no solo se trata de proteger al Estado de un ataque que comprometa el control sobre la infraestructura eléctrica de un centro poblado, sino que se debe proteger, por dar ejemplos, los datos de las personas que pueden sufrir cuando se dan fugas masivas de información en sectores esenciales como la salud, de evitar los impactos en una economía cuando se secuestra el sistema de suministro de gasolina en una región determinada, o de prevenir afectaciones a los derechos de la población si sucede un ciberataque que compromete las elecciones en un país democrático. Gestionar el riesgo nacional digital tiene como propósito proteger la seguridad nacional, pero va mucho más allá y su finalidad principal es la de apoyar la prosperidad económica y social, es pensar en la seguridad ciudadana y no solo de los estados.

También es necesario reflexionar cómo los más recientes escándalos mundiales sobre seguridad digital dan cuenta de la vulnerabilidad de determinados grupos poblacionales -especialmente defensores de derechos humanos, periodistas, activistas medioambientales, etcétera- a ataques que provienen del crimen organizado, pero también que son protagonizados por su propio Estado[13].

De otra parte, dado que se está regulando sobre asuntos de seguridad nacional, consideramos conveniente que la normatividad sobre este asunto se haga mediante una ley y mediando una discusión amplia en el Congreso. De esta forma, se lograría dar más garantías a la política, se ampliará la participación ciudadana y se generaría confianza en la política de gobernanza digital, este último, un parámetro indispensable cuando hablamos de gobernanza y seguridad en la web.

En suma, la promoción y protección de los derechos humanos como elemento central de cualquier política nacional de seguridad digital es central para que ésta aporte a la prosperidad económica y social y hay que hacer el esfuerzo por integrarlos, no solo mencionarlos en un rincón. Además, una política pensada desde los derechos humanos, sin dejar de ser efectiva, generaría confianza en las instituciones y los procedimientos implementados, tal como lo exige en Conpes 3995 de 2020.

Recomendación:

- La política nacional de seguridad digital debe ser consistente con los derechos humanos de las personas que busca proteger, solo así conseguirá construir

[13] https://en.wikipedia.org/wiki/Pegasus_Project_(investigation)

confianza y desarrollar una cultura coordinada de seguridad digital.
- Evaluar que el proceso de regulación no puede hacerse con un decreto, sino que requiere una ley.

1.3. El decreto propone un modelo desactualizado de abordaje para la política nacional de seguridad digital

Esta afirmación se soporta en dos observaciones. La primera, es que aunque la transformación digital, que ha hecho de la seguridad digital una importante necesidad, es muy compleja, y aunque el decreto tiene la ambición de asumir esta complejidad lo hace priorizando la seguridad nacional. En segundo lugar, aunque menciona el enfoque de análisis de riesgo, toda la norma está orientado a la seguridad de los sistemas.

El decreto no ha conseguido establecer qué es exactamente lo que hará: ¿será la política nacional de seguridad digital en seguridad nacional o será la política nacional de gestión del riesgo de seguridad digital? Si es el primero debe ser una ley y pensarse en cómo coordinar con otros sectores, pero renunciar a ser el gran líder cuando se trata de coordinar con otro. Si es el segundo le hace falta muchos elementos, como lo explicamos a continuación:

1.3.1. El Decreto se anuncia con cuatro propósitos “lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital”, pero su foco está en la seguridad nacional.

Aunque la memoria justificativa del futuro decreto solo menciona una vez -con una mención histórica al Conpes de 2011- y en el decreto dos veces a la seguridad nacional, es claro que la aproximación de este documento relaciona directamente la seguridad digital con la nacional y sin las claridades suficientes. Además su mirada es esencialmente técnica dejando de lado la complejidad del objetivo mayor que en palabras de la OCDE es la prosperidad económica y social, y en las nuestras poner en el centro a las personas para un desarrollo social integral. La propuesta del decreto es una mirada desactualizada del campo de impacto de la seguridad digital dando al Ministerio de Defensa mucho poder y control y en donde se administra el riesgo con inventarios estáticos de infraestructuras críticas, algo que en el panorama actual es insuficiente.

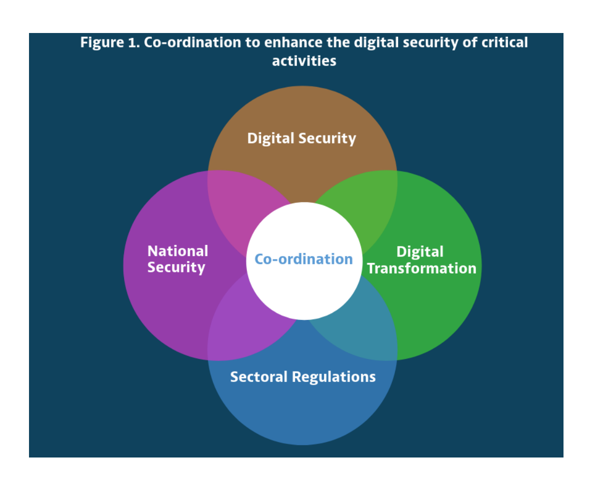
Hace una década la preocupación central de una política nacional de ciberseguridad (como se llamaba entonces haciendo énfasis en su carácter militar) era la seguridad nacional y la definición de las infraestructuras críticas para proteger al país de ataques cibernéticos. El temor era que el ingreso y control de los sistemas de suministro eléctrico de una ciudad o de una presa pusieran en riesgo la seguridad de la población o fueran usados como armas por otro país, por ejemplo.

El informe OCDE “Políticas de banda ancha para América Latina y el Caribe” en su capítulo 14, que habla de gestión del riesgo digital, cuando se refiere a los objetivos de una estrategia nacional se refiere a crear una política de gestión nacional del riesgo digital e indica expresamente que debe ser objetivo de esa política que “todas las partes interesadas

en este tema entiendan que el manejo de la gestión del riesgo es un desafío económico y social, **no simplemente un tema técnico o de seguridad nacional**" (resaltado nuestro).

Efectivamente, durante los últimos años la evolución de estas políticas nacionales, como se ve en los documentos OCDE, supone no sólo proteger la infraestructura crítica para hablar de la infraestructura informacional, sino, también, de la seguridad nacional para ocuparse de múltiples sectores.

La transformación digital amplía el impacto de la seguridad digital y complejiza el escenario actual. En este sentido la seguridad nacional es tan solo un aspecto. Así lo reconoce también las recomendaciones OCDE más recientes (2021) que buscan "Mejorar la seguridad digital de las actividades críticas"[14]. Las políticas de seguridad digital de las actividades críticas -el concepto OCDE actividades críticas equivale a servicios esenciales que es el que se usa en el decreto- se encuentran en la encrucijada de varios campos. La OCDE lo explican con la siguiente gráfica:



En ese mismo documento, la OCDE reconoce que hay un importante desafío de coordinación porque son muy diversas las agendas de política nacional (seguridad nacional, agenda de transformación digital, de seguridad digital, de otros sectores como el financiero, el de salud, transporte o comunicaciones). Además, señala que es necesario implementar un enfoque de coordinación basado en una evaluación nacional de riesgos. Y, sí, la protección de las infraestructuras críticas del país es clave y será parte de la agenda de seguridad nacional, pero no debe ser la totalidad de la misma. De igual forma, resulta contraproducente extrapolar las metodología de seguridad digital a otros ámbitos de la gobernanza digital, como lo hace el decreto.

El campo de seguridad nacional es un elemento central de las políticas de seguridad digital. Los Ministerios de Defensa son actores centrales y usualmente están a cargo de definir lo que se protege y cómo. Pero la presencia de la seguridad nacional en este campo, como en cualquier otro ambiente, supone unos poderes tan grandes e importantes que requiere no solo establecer el qué y el cómo, también se necesitan los controles y los mecanismos de rendición de cuentas. El propósito es construir confianza y evitar los abusos derivados de grandes poderes. El decreto no solo no es claro en decir que es la política nacional de seguridad nacional en seguridad digital sino que no desarrolla los mecanismos de control y seguimiento a esta actividad.

Mirando el gráfico de la OCDE reproducido previamente y después de leer el documento abierto a comentarios, lo que este documento hace esencialmente es abordar el tema desde la agenda de la seguridad nacional, con un importante énfasis en el inventario de

[14] https://goingdigital.oecd.org/data/notes/No17_ToolkitNote_DigitalSecurity.pdf

infraestructuras críticas y unos visos de coordinación especialmente en el tema de seguridad digital y haciendo un guiño hacia otros sectores, sin embargo, repetimos ese alcance no solo no es claro, tampoco es expreso.

El Decreto debe decidir si es la política de seguridad digital en la seguridad nacional y define elementos de coordinación o si es más amplia y tiene que establecer claramente esa extensión junto a los límites de la seguridad nacional. Si es sobre seguridad nacional es el Congreso el que debe continuar para delimitar claramente lo que es de carácter civil, las vías castrenses y evitando empoderar injustificadamente al Ministerio de Defensa nacional frente a sujetos de derecho privado.

El borrador de decreto colombiano tiene algunos guiños de evolución de la visión militarista y de seguridad nacional a un panorama más complejo: se le da un papel más protagónico al Ministerio TIC, se incorpora a múltiples entidades públicas en el principal cuerpo de gobernanza, se habla de un enfoque de análisis de riesgo y se transfiere al ColCERT del Ministerio de Defensa al ministerio TIC.

Sin embargo, esto no alcanza para que el documento presentado pueda pasar como la política nacional de seguridad digital que debiera ser entonces la de gestión del riesgo digital.

1.3.2. El borrador de decreto no consigue desarrollar el enfoque del análisis de riesgo, se queda en el ya internacionalmente superado enfoque de seguridad de los sistemas y redes de información

El documento que acompaña y explica las “Recomendaciones del Consejo sobre la gestión de riesgos de seguridad digital para la prosperidad económica y social”[15] de la OCDE de 2015 explica que el principal cambio en los principios que recoge es el de reorientar el enfoque de la "seguridad de los sistemas y redes de información" hacia el de “riesgo de seguridad para las actividades económicas y sociales que dependen del entorno digital”.

Por su parte el informe OCDE “Políticas de banda ancha para América Latina y el Caribe” en su capítulo 14 tiene un diagnóstico muy concreto para nuestra región, señala que se requiere “desarrollar una estrategia nacional para la gestión de los riesgos de seguridad digital”, que describen así:

> “**Desarrollar una estrategia nacional para la gestión de los riesgos de seguridad digital**. Las estrategias nacionales para la gestión de los riesgos de seguridad digital deben tener como objetivo promover la prosperidad económica y social. Deben coordinarse ampliamente dentro del gobierno para garantizar la coherencia con otras estrategias para la prosperidad económica y social, y la coherencia con las políticas destinadas a proteger las infraestructuras críticas y garantizar la prestación de servicios esenciales. El objetivo es combatir la criminalidad, proteger la seguridad nacional y preservar la estabilidad internacional. Estas estrategias deben ser apoyadas al más alto nivel de gobierno, para garantizar que los diversos intereses en juego estén debidamente equilibrados. Deben ser flexibles y tecnológicamente neutras y, mientras tanto, preservar y proteger los derechos humanos y los valores fundamentales.”

El enfoque del decreto sometido a consideración aunque menciona implementar el enfoque de análisis de riesgos, lo deja en un rincón, no lo desarrolla. El decreto apuesta y desarrolla

[15] https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf ver el BOX 2

el enfoque de redes y sistemas de información. Por eso es claro que también acá dice una cosa y hace otra, adopta una aproximación desactualizada.

El propio documento que acompaña y explica las Recomendaciones de la OCDE de 2015 sobre riesgos de seguridad digital mencionados, habla de que en el sector en el que hoy el enfoque que se aplica es el de gestión del riesgo. Las palabras exactas en el documento explicativo de las Recomendaciones OCDE de 2022 es que

> “la definición de diccionario de "seguridad" - "el estado de estar libre de daño o peligro"- sugiere un objetivo binario y estático inherentemente en contradicción con el concepto de gestión de riesgos. Para algunos, la "seguridad" se relaciona con la "seguridad nacional", un ámbito a menudo asociado, con razón o sin ella, a una cultura en la que la "seguridad" es primordial por encima de cualquier otra consideración. Así, a diferencia de las Directrices de Seguridad de 2002, la seguridad" como un adjetivo que caracteriza el riesgo, los factores de riesgo y el enfoque de la gestión del riesgo, y no como un sustantivo que señala un objetivo independiente.”

A pesar de los esfuerzos del borrador del decreto por adoptar un modelo actualizado de política nacional de seguridad digital el resultado es anticuado y no cumple con los estándares propuestos por la OCDE:

Recomendación:

- El borrador de decreto tiene que definir claramente su alcance y desarrollarlo superando las visiones anticuadas de priorizar la seguridad nacional y su enfoque de seguridad de los sistemas y las redes de información.
- Esta regulación debe decidir si es una política nacional de seguridad digital para la seguridad nacional o si es la política nacional para la gestión del riesgo digital que coordina los diferentes sectores.
    - Si el decreto es la política nacional de seguridad nacional debe ser una ley que se discute en el Congreso.
    - Si el decreto busca unos lineamientos amplios -como lo sugiere el título- el decreto debe reorientar el enfoque de "seguridad de los sistemas y redes de información" y convertirse en la política nacional de gestión del riesgo de seguridad digital que coordinará todos los sectores, con la prelación que corresponda a los temas de seguridad nacional.

2. Comentarios específicos

Aunque consideramos que es necesario modificar sustancialmente el documento presentamos algunos comentarios específicos adicionales. Dada la premura del tiempo otorgado para comentarios en algunas ocasiones podemos dar más detalles, en otras menos.

2.1. No basta con mencionar en el último de los principios que se pretende la salvaguarda de los derechos humanos y los valores fundamentales de los ciudadanos para cumplirlos.

Comentario

En nuestra cultura jurídica, hablando de ciberseguridad, no es claro lo que se entiende por “valores fundamentales”. Por lo tanto, en el decreto se debe acentuar en defensa de los

derechos humanos. Y si se desea, se deben describir los valores fundamentales a los que se refiere el artículo sobre los principios, sobre todo, si estos se desarrollan en un contexto como el colombiano. Por tanto, se propone el siguiente cambio.

Texto actual

ARTÍCULO 2.2.21.1.1.5. *Principios. Además de los principios previstos en los artículos 209 de la Constitución Política, 2° de la Ley 1341 de 2009, 3° de la Ley 1437 de 2011, 4° de la Ley 1581 de 2012 y los atinentes a la Política de Gobierno Digital contenidos en el artículo 2.2.9.1.1.3 del Decreto 1078 de 2015, a los efectos del presente decreto se aplicarán los siguientes:*

11. Salvaguarda de los derechos humanos y los valores fundamentales de los ciudadanos. En la aplicación e interpretación de los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la gestión de riesgos de Seguridad Digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, y la respuesta a incidentes de Seguridad Digital del sector gobierno de Colombia, se respetarán los derechos humanos y valores fundamentales incorporados en la Constitución Política y los tratados internacionales ratificados por Colombia.

Propuesta

Que se modifique el texto del **ARTÍCULO 2.2.21.1.1.5. *Principios*** y cambie el orden de los principios establecidos, de forma tal que los principios de proporcionalidad, inclusión y salvaguarda de los derechos humanos sean los primeros. Además que se agregue el siguiente texto:

ARTÍCULO 2.2.21.1.1.5. *Principios.* *Además de los principios previstos en los artículos 209 de la Constitución Política, 2° de la Ley 1341 de 2009, 3° de la Ley 1437 de 2011, 4° de la Ley 1581 de 2012 y los atinentes a la Política de Gobierno Digital contenidos en el artículo 2.2.9.1.1.3 del Decreto 1078 de 2015, a los efectos del presente decreto se aplicarán los siguientes:*

1. **Salvaguarda de los derechos humanos**. Promover el desarrollo económico y social, y lograr un Internet libre, abierto, seguro e inclusivo supone un compromiso con la salvaguarda de los derechos humanos de las personas, protegiendo especialmente la libertad de expresión, el derecho a la información, el de la intimidad, el habeas data y la protección de datos, y promoviendo los valores democráticos y del Estado de Derecho. En caso de limitación a estos derechos, debe ser bajo medidas excepcionales y estar conforme con la Constitución Política y los estándares internacionales aplicables. Estas medidas, deben ser proporcionales, necesarias y darse en un marco de legalidad.

2.2. Consideramos positivo para hacer efectiva la protección de los derechos humanos que el Colcert pase al control del MinTIC

Fundación Karisma había señalado con antelación[16] al Estado colombiano y así fue reseñado por la Organización para la Cooperación y el Desarrollo Económicos (OCDE)[17], la necesidad de que el Grupo de Respuestas a Emergencias Cibernéticas en Colombia (ColCERT) dejara de hacer parte del Ministerio de Defensa. Esto debido a que el ColCERT debe recibir información sobre incidentes o vulnerabilidades y el hecho de que esté vinculado al Ministerio de Defensa puede representar un desincentivo para muchas personas activistas, defensoras de derechos humanos o hackers éticos a la hora de reportar una vulnerabilidad o incidente[18]. Además, el que el ColCERT hiciera parte del Ministerio de Defensa le daba un enfoque ofensivo o militarista a dicha entidad.

Siendo así, consideramos un acierto del decreto de ciberseguridad que en adelante el Ministerio de Tecnologías de la Información y las Comunicaciones sea encargado de coordinar al ColCERT y de establecer sus funciones y forma de funcionamiento. Este es el mejor ejemplo de cómo las acciones de una política nacional pueden en la práctica aplicar la obligación de proteger los derechos fundamentales de las personas.

Propuesta Fortalecer el ColCERT con mecanismos de coordinación con múltiples partes interesadas, mecanismos coordinados de respuesta a vulnerabilidades como se explicará más adelante.

2.3. Comentarios sobre las definiciones y conceptos usados en el secreto de ciberseguridad

2.3.1. La definición de seguridad digital debe estar en línea con los derechos humanos

Comentario

Con base en los comentarios generales ya realizados, la simple lectura de la definición de seguridad digital usada en el decreto permite concluir que estamos frente a un concepto militar donde predominan términos como normalidad o ciberdefensa, y no se usan expresiones como: gestión del riesgo y múltiples partes interesadas las cuales son más actuales teniendo en cuenta la evolución que ha habido en la materia. El decreto en este aspecto no sigue los lineamientos OCDE[19].

Por esta razón, invitamos a revisar la definición para que refuerce la relación entre seguridad digital y derechos humanos, punto clave para promover un ciberespacio seguro y libre. En ese sentido, insistimos -como lo hemos hecho en comentarios a los Conpes del pasado- que la definición propuesta por el Grupo de Trabajo 1 (WG1, por sus siglas en inglés) de la Freedom Online Coalition (FOC) presenta un buen balance al respecto y, tal vez, pueda servir de guía[20].

---

[16] https://web.karisma.org.co/wp-content/uploads/download-manager-files/RutasDeDivulgacion.pdf
[17] https://one.oecd.org/document/DSTI/CDEP/SDE(2020)3/FINAL/en/pdf
[18] https://web.karisma.org.co/aportes-para-un-entorno-seguro-y-confiable/
[19] https://goingdigital.oecd.org/data/notes/No17_ToolkitNote_DigitalSecurity.pdf
[20] FOC-WGl. (2014). Recommendations for Fluman Rights Based Approaches to Cybersecurity.

Texto actual

Seguridad digital: Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), a través de la apropiación de políticas y buenas prácticas y mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas.

Propuesta

Que se elimine la definición de Seguridad digital del **Artículo 2.2.21.1.1.3.** ***Definiciones*** *y en su lugar se establezca la siguiente:*

Seguridad digital es la preservación, a través de políticas, tecnología y educación, de la disponibilidad, confidencialidad e integridad de la información y su infraestructura subyacente a fin de mejorar la seguridad de las personas tanto online como offline.

Alternativamente se puede ajustar la definición de OCDE:

Seguridad digital: es un reto económico y social y no sólo una cuestión técnica, se trata de un conjunto de medidas para gestionar el riesgo de la seguridad digital para la prosperidad económica y social, para la garantía de derechos humanos y la promoción de los valores democráticos.

2.3.2. La definición de servicios esenciales es vaga, ambigua, muy amplia

Comentario y texto actual
El decreto correctamente va más allá de la infraestructura crítica para incorporar el concepto más amplio de "servicios esenciales", pero no consigue darle foco. La definición es demasiado amplia y aunque reconoce una visión de prosperidad económica y social no la desarrolla. Sobre este punto, la guía "Going digital" de la OCDE[21], ofrece información importante:

> "la noción de infraestructura crítica surgió a finales de la década de 1990, cuando algunos países de la OCDE comenzaron a adoptar políticas de protección de infraestructuras críticas (PIC). Estas políticas solían tener en cuenta sectores de infraestructuras críticas como la energía, finanzas, telecomunicaciones o salud pública.
>
> Progresivamente, la necesidad de desarrollar políticas para proteger los sistemas de información y de información que apoyan a estos sectores de infraestructuras críticas fue cada vez más clara. En torno a 2008, pareció natural denominar a estos activos de las TIC "infraestructuras críticas información" (ICI), como si formaran un sector adicional de infraestructuras críticas. Sin embargo, aunque es bastante popular entre los expertos el concepto de ICI rara vez se ha utilizado para desarrollar marcos políticos nacionales. Esto puede deberse a la dificultad de delimitar las ICI en la práctica. Por ejemplo, Internet puede considerarse parte de las ICI porque la mayoría de los operadores de otras infraestructuras críticas dependen de ella, como

[21] https://goingdigital.oecd.org/data/notes/No17_ToolkitNote_DigitalSecurity.pdf

los bancos, los hospitales o los distribuidores de energía. Sin embargo, estos operadores también dependen de sus sistemas y redes de información críticos internos, que por tanto son sistemas y redes de información críticos internos, que por tanto también forman parte de las ICI.

Algunas partes de estos sistemas y redes de información pueden ser internas para los operadores de infraestructuras críticas, es decir, "en las instalaciones", pero otras pueden estar "en la nube", es decir, en Internet, y ser propiedad de terceros y estar gestionadas por ellos, potencialmente en otras jurisdicciones. Esta combinación de componentes técnicos compartidos y aislados, así como internos y externos, hace que las ICI sean difíciles de representar y más complejas que los sectores de "infraestructuras críticas" más tradicionales en los que se inspiró el concepto de ICI. En 2019, la OCDE acordó simplificar el marco establecido en su Recomendación de 2008 sobre la protección de las infraestructuras críticas de información, centrándose en la necesidad de mejorar la seguridad digital de las actividades críticas, es decir, animar a los operadores de actividades críticas a gestionar mejor el riesgo de seguridad digital."

Es importante entonces que la política sea clara sobre la diferencia entre infraestructura crítica y cuando se pasa a la capa de información que corresponde actualmente al concepto de actividades críticas o servicios esenciales. La misma guía "going digital" indica que "La noción de actividad crítica (a veces denominada funciones críticas o servicios esenciales) es diferente de la de infraestructura crítica porque se centra en el riesgo para la prestación del servicio y no para los activos en los que se basa la prestación del servicio".

El siguiente cuadro muestra cómo el decreto define infraestructura crítica y servicios esenciales, y cómo la OCDE define actividad crítica:

Definición del decreto Texto actual **Infraestructura crítica cibernética**	Definición del decreto Texto actual **Servicios esenciales**	Definición de OCDE en la guía "going digital" sobre la seguridad digital de las actividades críticas Propuesta **Actividad crítica**
Son las infraestructuras estratégicas soportadas por Tecnologías de la Información y las Comunicaciones (TIC) o Tecnologías de Operación (TO), cuyo funcionamiento es indispensable, por lo que su suspensión, afectación, o destrucción tendría un grave impacto o efecto perturbador sobre los servicios esenciales del Estado.	Es el servicio necesario para el mantenimiento de las actividades sociales y económicas del país, que dependen del uso de tecnologías de la información y las comunicaciones, y un incidente en su infraestructura o servicio podría generar un daño significativo que afecte la prestación de dicho servicio y la consecuente parálisis de las actividades.	Una actividad crítica es una actividad económica y social cuya interrupción o perturbación tendría graves consecuencias para la salud, la seguridad y la protección de los ciudadanos; o el funcionamiento eficaz de los servicios esenciales para la economía y la sociedad, y del gobierno; o la prosperidad económica y social en general (OCDE, 2019[4]). Este último tipo de actividades críticas incluye aquellas que son esenciales para la prosperidad sin ser

		necesariamente críticas para el funcionamiento de la economía y la sociedad, ni afectar a la salud, la seguridad y la protección de los ciudadanos. Por ejemplo, la fabricación de automóviles o la minería, en un país en el que estas actividades representen una parte importante del PIB.

En el decreto no basta con definir por aparte la infraestructura crítica y los servicios esenciales, es importante que la definición explique de qué se habla y que la forma como se protege aborde sus características. Una simple mirada a la definición de servicios esenciales del decreto con el de actividades críticas de la OCDE muestra que hay mucho más a pensar en ese concepto y puede explicar la visión tan desactualizada que tiene

Propuesta

Que se elimine la definición de servicio esencial del **Artículo 2.2.21.1.1.3. *Definiciones***, *y en su lugar se establezca la siguiente:*

Un servicio esencial. Es una actividad económica y social cuya interrupción o perturbación tendría graves consecuencias para la salud, la seguridad y la protección de los ciudadanos; o el funcionamiento eficaz de los servicios esenciales para la economía y la sociedad, y del gobierno; o la prosperidad económica y social en general.

Incluye las actividades que son esenciales para la prosperidad sin ser necesariamente críticas para el funcionamiento de la economía y la sociedad, ni afectar a la salud, la seguridad y la protección de los ciudadanos. Por ejemplo, la fabricación de automóviles o la minería, en un país en el que estas actividades representen una parte importante del PIB.

2.3.3. Actualizar la definición de gobernanza de la seguridad digital

Comentario

Como ya se explicó se debe actualizar el enfoque de sistemas de información, infraestructura tecnológica, redes e información y asumir el enfoque de análisis del riesgo digital. Todo lo dicho en los comentarios generales obligan a una revisión integral del decreto y hacen que la definición actual se vea vaga.

El decreto en este aspecto no sigue los lineamientos OCDE[22], no está asignando responsabilidades y es insuficiente en la medida en que en la práctica el decreto termina asignando demasiado poder al Ministerio de Defensa y por tanto ignora la complejidad del espacio de transformación digital.

[22] https://goingdigital.oecd.org/data/notes/No17_ToolkitNote_DigitalSecurity.pdf

Si bien consideramos que la gobernanza no debería definirse, sino implementarse, también creemos que si se va a definir una forma de hacerlo no es con palabras bonitas que luego no se desarrollan -y que contienen conceptos desactualizados- sino enunciando las características que la OCDE en sugirió en 2021[23]. Sobre el modelo de gobernanza hablaremos más adelante.

En todo caso, una gobernanza efectiva de la seguridad digital debe estar alineada con las metas del país y debe asegurar que sus acciones y actividades estén en línea con los derechos humanos y las libertades de la población.

Texto actual
Gobernanza de la seguridad digital para Colombia: Se refiere a los enfoques utilizados por múltiples partes interesadas para identificar, enmarcar, proponer, y coordinar respuestas proactivas y reactivas a posibles amenazas a la confidencialidad, integridad o disponibilidad de los servicios tecnológicos, sistemas de información, infraestructura tecnológica, redes e información que en conjunto constituyen el entorno digital.

Propuesta

Que se elimine la definición de Gobernanza de la seguridad digital para Colombia del **Artículo 2.2.21.1.1.3. *Definiciones***, *y en su lugar se establezca la siguiente:*

Gobernanza de la seguridad digital para Colombia: Se refiere al modelo que en conjunto con una metodología práctica se usa para definir e implementar los tres elementos esenciales para el manejo de amenazas relacionadas con el entorno digital: 1) Adoptar al más alto nivel del gobierno, y como parte de una estrategia nacional de seguridad digital, objetivos claros para reforzar la seguridad digital, definir el apetito de riesgo y la resistencia de los servicios esenciales, 2) Adoptar un mecanismo de gobernanza nacional que asigna responsabilidades a organismos gubernamentales tanto operativamente como en la toma de decisiones para mejorar la seguridad digital de los servicios esenciales dentro y entre sectores, y 3) garantiza una coordinación nacional de todo el gobierno para establecer la cooperación intergubernamental, garantizar la coherencia de las medidas adoptadas en todos los sectores, asignar recursos entre los organismos gubernamentales responsables y crear una masa crítica de conocimientos y habilidades, y facilitar la cooperación transfronteriza.

2.3.4. La definición de gestión de riesgo es totalmente vaga e insuficiente

Comentario
Como ya lo explicamos, el análisis y gestión de riesgo en el decreto es mencionado sin mayor desarrollo a pesar de que la gestión de los riesgos de seguridad digital es la metodología clave para abordar la complejidad de la actividad crítica (que en el decreto se llama servicios esenciales). Por lo tanto, se deben integrar los lineamientos de la OCDE, especialmente los descritos en la guia “mejorando la seguridad digital de las actividades críticas”[24] y en la guía “going digital”.

[23] https://goingdigital.oecd.org/data/notes/No17_ToolkitNote_DigitalSecurity.pdf
[24] https://goingdigital.oecd.org/data/notes/No17_ToolkitNote_DigitalSecurity.pdf

El texto actual no aborda este desafío. Debemos empezar por definir los riesgos digitales y la gestión de los riesgos digitales. Recomendamos analizar los textos propuestos por la OCDE en la guía “mejorando la seguridad digital de las actividades críticas” que además no es solo un tema de los sujetos obligados sino que debiera ser el enfoque de una política nacional de gestión de riesgo. La definición actual no habla de una metodología (que es lo que es la gestión del riesgo) sino más de una aspiración.

Lo correcto debería ser definir el riesgo digital e implementar el enfoque de gestión del riesgo, pero esto supone un cambio sustancial de decreto en la forma como está actualmente. Sugerimos adaptar las definiciones dadas por la OCDE en 2021[25].

Texto actual
Enfoque basado en la gestión de riesgos. Los sujetos obligados deben gestionar el riesgo de forma que el uso de tecnologías de la información y las comunicaciones fomente la confianza en el entorno digital, la prosperidad económica y social, genere riqueza, innovación, productividad, competitividad, y empleo en todos los sectores de la economía, y ello no suponga la materialización de infracciones a los derechos de los ciudadanos.

Propuesta

Que se elimine la definición de Riesgo de seguridad y Enfoque basado en la gestión de riesgos de seguridad del **Artículo 2.2.21.1.1.3.** ***Definiciones****, y en su lugar se establezca las siguientes definiciones:*

Riesgo de seguridad digital: es el efecto perjudicial que los incidentes de seguridad digital pueden tener en las actividades económicas y sociales. Es la combinación de la probabilidad de que los incidentes de seguridad digital afecten a una actividad económica y social con la gravedad de las consecuencias que dichos incidentes pueden crear para las partes interesadas. Es también un reto económico y social causado por la posibilidad de que se produzcan incidentes a nivel técnico. Los aspectos técnicos de los incidentes de seguridad -como el uso de malware, phishing y otras técnicas, la corrupción de datos, indisponibilidad de servidores, violaciones de la confidencialidad, etc- no deben ocultar la naturaleza económica y social del riesgo.

Enfoque basado en la gestión de riesgos de seguridad digital. es la metodología para seleccionar medidas de seguridad que sean adecuadas y proporcionales al riesgo, que estén alineadas con la tolerancia al riesgo, apoyen las actividades económicas y sociales en juego y no perjudiquen estas actividades, por ejemplo, cerrando indebidamente el entorno o limitando la posibilidad de aprovechar las tecnologías de la información y las comunicaciones para fomentar la confianza en el entorno digital, la prosperidad económica y social, la generación de riqueza, la innovación, productividad, competitividad, y empleo en todos los sectores de la economía, y la promoción y protección de los derechos humanos.

2.3.5 La definición de incidente de seguridad digital es vaga e insuficiente.

Comentario:

[25] https://goingdigital.oecd.org/data/notes/No17_ToolkitNote_DigitalSecurity.pdf

Los incidentes de seguridad digital no solo afectan actividades en el entorno digital como lo define el decreto, sino que pueden traspasar esa digitalidad y afectar infraestructura o procesos que podríamos enmarcar en lo físico. Incidentes como el de Stuxnet que inhabilitó centrífugas nucleares en Irán, los cortes de energía en 2015 y 2017 en Ucrania, los mas recientes ataques de ransomware a empresas de transporte como Maersk o los ataques que dejaron por fuera de funcionamiento el gasoducto Colonial en Estados Unidos en 2021 dan cuenta de que la definición de incidente de seguridad digital va mucho más allá de las actividades meramente digitales y pueden fácilmente pasar a un daño físico que afecte las cadenas de suministro, los sistemas de defensa y la prestación de servicios esenciales como el suministro de combustibles, energía o agua, entre otros.

En este sentido, recomendamos adoptar la definición de la OCDE que integra el concepto de la triada AIC (Availability, Integrity and Confidentiality) a todas las actividades que de alguna manera están conectadas o dependen de hardware, software, redes o datos que las soportan. Por otro lado, la definición del decreto da cuenta de que cualquier evento adverso intencionado o no, es un incidente de seguridad digital, lo cual incluiría, por ejemplo, desastres naturales que claramente no son incidentes de seguridad digital.

Texto actual:
Incidente de seguridad digital: cualquier evento adverso intencionado o no intencionado, que puede cambiar o afectar el curso esperado de una actividad en el entorno digital.

Propuesta:

Que se elimine la definición actual de Incidente de seguridad digital del **Artículo 2.2.21.1.1.3.** ***Definiciones****, y en su lugar se establezca la siguiente:*

Incidente de seguridad digital: Es un evento relacionado con los riesgos de seguridad digital que puede interrumpir la disponibilidad, integridad y confidencialidad (triada AIC) del hardware, software, redes o datos que soportan actividades económicas y sociales.

2.4. Operadores supeditados al Ministerio de Defensa y la impertinencia de un inventario estático.

Comentario

La definición de lo que se debe proteger en la propuesta de decreto queda a cargo del Ministerio de Defensa, a quien se dan amplios poderes para definir qué es objeto de su cuidado y supervisión a través de la construcción de un inventario. Para la OCDE establecer el cómo se va a decidir qué es lo que se va a proteger es un elemento clave de la definición de las políticas nacionales de seguridad digital cuando se habla de actividades críticas (servicios esenciales según el decreto) y la definición depende precisamente de la implementación de un enfoque de gestión nacional del riesgo (aproximación dinámica), nada más opuesto a lo que el decreto en comento prevé, un inventario (aproximación estática).

Un enfoque de gestión de riesgo digital supone mejorar la seguridad digital de las actividades críticas y gira en torno a convencer a las entidades públicas y privadas de

mejorar la gestión del riesgo y coordinarla. Para la OCDE en la mencionada guía “mejorando la seguridad digital de las actividades críticas”[26]:

> “si se aplica a demasiados operadores se impondrán barreras a la economía (agregamos: a la actividad social y ejercicios de derechos también) y si se aplica a muy pocos, no se estaría protegiendo la economía”.

En esta afirmación está el sesgo de la OCDE hacía la economía, pero algo parecido pasará en general con los temas sociales y no deben ser desconocidos.

Hay diferentes aproximaciones para decidir cómo hacerlo en los diferentes países, pero la OCDE aconseja que se haga trabajando con los actores públicos y privados, con las partes interesadas. El enfoque de gestión de riesgo digital para la OCDE supone trabajar con las partes interesadas que incluyen:

- El operador de la actividad cuyos activos operativos, físicos financieros o de reputación puedan verse afectados (por ejemplo, las centrales eléctricas de una compañía de una compañía eléctrica);
- Las empresas, los gobiernos y los individuos que dependen de la prestación de la actividad que se vea interrumpida, como clientes o usuarios (por ejemplo, ciudadanos afectados por el apagón resultante);
- La sociedad en general, como cuando la escala de la interrupción es muy grande (por ejemplo, todas las actividades económicas se ven afectadas en la región, o la interrupción se extiende a otros sectores como transporte o la atención sanitaria).

Para La OCDE, la definición de lo que se protege debe ser el resultado de un enfoque intergubernamental coordinado, de un proceso abierto y transparente en el que participen todas las partes interesadas. Y, atención, debe ser revisado y mejorado periódicamente sobre la base de la experiencia y las mejores prácticas, utilizando métricas comparables a nivel internacional cuando estén disponibles[27].

El decreto no sigue estos parámetros, le entrega demasiado poder al Ministerio de Defensa que es quien define el inventario y adquiere poderes de supervisión sobre una de las partes interesadas en el proceso claves, los operadores -de esto hablaremos en el siguiente punto-. Esta facultad exagerada por supuesto ni es un esfuerzo coordinado, ni es abierto, ni mucho menos transparente.

2.4.1. En lugar de una aproximación que convence a los operadores de participar en el proceso, escogieron una que los obliga, esto es la garantía del desastre.

El decreto no es preciso sobre la naturaleza y alcance de las medidas que deben tomar los operadores de actividades críticas, la ambigüedad genera dudas frente al rol de supervisión del Ministerio de Defensa y tampoco permite establecer cuál es el modelo que adoptamos en Colombia, el texto justificativo de la norma no informa sobre los pros y contras tampoco.

La OCDE ha indicado que la evolución hacia los conceptos de actividades críticas y enfoque de gestión de riesgo digital supone que las políticas nacionales deban asignar responsabilidades a los operadores. Indica la OCDE que la forma como se da esta

[26] https://goingdigital.oecd.org/data/notes/No17_ToolkitNote_DigitalSecurity.pdf
[27] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0415

regulación a nivel internacional es muy variable, desde regulaciones que imponen obligaciones (Europa) hasta autoregulaciones y recomendaciones (EE.UU. o Japón), pero todas coinciden en solicitar mejoras en la gestión del riesgo y compartir información sobre riesgo, mejores prácticas y respuesta a incidentes como mínimo. De esta forma el dinamismo y la gobernanza de múltiples partes interesadas ayudan a integrar actores muy diferentes que son parte de un entorno complejo donde se desarrolla la seguridad digital.

La OCDE advierte que el reto de los gobiernos es el dinamismo de las tecnologías digitales, el desafío lo manejan las regulaciones de manera muy diferente. En Colombia no lo estamos haciendo, el Decreto prioriza la seguridad nacional sacrificando el reconocimiento de un entorno más complejo y su enfoque no es gestión de riesgos sino el de sistemas de información, infraestructura tecnológica y las redes e información que le apuesta a la construcción de un inventario de infraestructura críticas cibernéticas nacionales y de servicios esenciales y gira en torno a unos operadores que serán monitoreados por el Ministerio de Defensa. Todo en contravía de los estándares de la OCDE que hablan de generar confianza, de convencer a las partes interesadas en el proceso, abrirles espacio de participación y usar educación y capacitación ampliamente. No solo la aproximación del decreto compromete la efectiva participación de estas entidades, compromete además el ecosistema, sin justificación crea una dependencia de privados al Ministerio de Defensa.

La necesidad de tener una visión dinámica del sector, que es la que promueve la OCDE, en la política nacional colombiana no existe. La apuesta, enfoques, definiciones y visión del decreto es estática.

En este contexto el decreto de ciberseguridad termina imponiendo obligaciones y responsabilidades a los sujetos de derecho privado obligados (operadores de servicios esenciales) y que serán monitoreadas por el Ministerio de Defensa Nacional incluso si dentro de la definición de servicio esencial están las actividades sociales y económica abriendo un espectro demasiado amplio de control. Este alcance tan amplio para señalar quienes están o no obligados por una norma puede generar inseguridad jurídica o implicar una vulneración al principio de legalidad y derecho al debido proceso (Constitución Política, Art 29).

Efectivamente la sección 4 del decreto de ciberseguridad establece la obligación de crear un inventario de infraestructuras críticas cibernéticas nacionales y de servicios esenciales, así como de sus responsables o prestadores. Esto con el objetivo de establecer qué entidades de derecho privado están obligadas a implementar las políticas de seguridad digital del Estado y por ende que quedan bajo supervisión del MinDefensa.

2.4.2. Sobre el inventario, una solución estática a un problema en movimiento.

Si bien tiene sentido que el inventario sobre la infraestructura cibernética y, en ese sentido, la de los prestadores de servicios del país quede a cargo de un Ministerio Defensa, no puede ser el abordaje cuando se trata de hablar de servicios esenciales o actividades críticas. En ese caso ni la metodología puede ser la de inventario y la definición estática de responsables, ni puede estar a cargo del Ministerio de Defensa (este organismo podrá tener un rol importante pero no puede ser el único).

Reiteramos que la ambigüedad y amplitud del decreto hace que asignar funciones sobre organizaciones privadas al MinDefensa da un enfoque policivo o belicista a la política de gobernanza digital. Esto no significa que en casos graves de incidentes de ciberseguridad será necesario la intervención del MinDefensa, sino que da cuenta de las falencias del

decreto y la necesidad de hablar de una ley para definir el alcance de la política nacional como se explicó en los comentarios generales.

Tema aparte merece una alerta final: debe tenerse en cuenta que al momento de que el Estado ratificó el Convenio de Budapest el Estado Colombiano señaló qué entidades quedaban encargadas de la coordinación de la política nacional y la cooperación a nivel internacional, siendo los señalados el Ministerio de Justicia y la Fiscalía[28]. Por lo tanto, deben eliminarse las facultades en la materia entregadas a Mindefensa.

Propuesta

Si la política nacional que estamos discutiendo es la del sector de seguridad nacional esta visión requiere ajustes -sobre todo en el terreno de controles y seguimiento a estas actividades- pero tiene sentido.

Si es la política nacional de seguridad digital el Ministerio de Defensa no puede ser el único encargado de la definición de un inventario, ni por vía de la amplia vaguedad del decreto puede quedar con poderes de supervisión sobre entes privados.

El Decreto debe establecer un mecanismo intergubernamental en el que participen las múltiples partes interesadas y definan lo que se protege aplicando un enfoque de gestión del riesgo digital.

El cambio que sugerimos es sustancial en lo relacionado con operadores y obliga a cambiar de fondo todas las previsiones relacionadas con este tema en el Decreto, el tiempo dado para comentar no permite ofrecer una propuesta para este cambio.

En relación con el tema del inventario como mínimo sugerimos revisar los artículos **Artículo 2.2.21.1.4.1.** y **Artículo 2.2.21.1.4.2.**

Dado que la coordinación de la política nacional y la cooperación a nivel internacional en línea con el Convenio de Budapest corresponde al Ministerio de Justicia y la Fiscalía es necesario asignar responsabilidades claras y asegurarse de que sin ambigüedades esto no corresponda a facultades asignadas al Ministerio de Defensa.

2.5. La propuesta de gobernanza del decreto de ciberseguridad es insuficiente para los objetivos que persigue.

En línea con los comentarios generales, las políticas nacionales de seguridad digital deben abordar la complejidad de coordinar diversos sectores con intereses y regulaciones muy variadas. Las recomendaciones OCDE más recientes (2021) que buscan "Mejorar la seguridad digital de las actividades críticas"[29] se ocupa extensamente del tema de gobernanza y vale la pena reproducir acá una buena parte (traducción propia):

> "No existe un enfoque único para la coordinación de todo el gobierno en los países de la OCDE. Los marcos de gobernanza varían considerablemente, en parte debido a las disposiciones constitucionales, al estilo de gobierno y a la estructura

[28] https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=0

[29] https://goingdigital.oecd.org/data/notes/No17_ToolkitNote_DigitalSecurity.pdf

administrativa de cada país. En todos los casos, los marcos de gobernanza deben garantizar la coherencia con los derechos humanos y los valores fundamentales.

La gobernanza se refiere generalmente a tres funciones claves: 1) la definición del marco político global o estrategia, 2) la aplicación del marco en cada sector y 3) la capacidad operativa. Las tres funciones pueden estar centralizadas en un único organismo, como en Francia (la Agencia Nacional de Seguridad de los Sistemas de Información, ANSSI), o distribuidas de diferentes maneras.

Por ejemplo, el desarrollo de la estrategia puede ser dirigido por un departamento o ministerio (por ejemplo, Alemania, Reino Unido, Japón), la capacidad operativa puede estar ubicada en una agencia independiente (por ejemplo, NCSC en el Reino Unido, la Oficina Federal de Seguridad de la Información (BSI) en Alemania, NISC en Japón), y la aplicación del marco y la supervisión puede estar centralizada o descentralizada a través de reguladores sectoriales (Recuadro 4). En Dinamarca, el marco político general fue desarrollado por el Ministerio de Finanzas como parte de la estrategia nacional de seguridad digital, pero cada Ministerio responsable de un sector crítico (energía, sanidad, transportes, etc.) debe debe desarrollar una subestrategia específica en su ámbito de competencia (Danish Ministerio de Finanzas, 2018[21]). En muchos países, el organismo encargado de asistencia operativa en materia de seguridad digital puede servir de enlace con las fuerzas de seguridad y órganos de inteligencia.

Cada enfoque tiene pros y contras. Por ejemplo, un enfoque centralizado facilita la coherencia de la normativa, pero dificulta la regulación sectorial detallada de los sectores, ya que requiere que el organismo central consulte a los reguladores sectoriales pertinentes y cree vínculos con los operadores privados de actividades críticas. y crear vínculos con los operadores privados de actividades críticas. Un enfoque descentralizado facilita el desarrollo y la aplicación de la normativa sectorial, pero requiere más esfuerzos para garantizar la coherencia entre los sectores y proporcionar al gobierno una comprensión holística de la situación. Una ventaja clave del enfoque descentralizado es que los reguladores sectoriales ya entienden sus limitaciones. Sin embargo, los operadores pueden ser reacios a revelar información relacionada con la seguridad digital a los reguladores sectoriales. que podría utilizarse para otros fines regulatorios (Comisión Europea, 2019[22]).

Un aspecto importante es la necesidad de garantizar que el organismo (o los organismos) responsable tiene (o tienen) suficiente capacidad para cumplir sus tareas, incluyendo financiación y recursos, así como experiencia en seguridad digital, que es escasa en la mayoría de los países y difícil de retener en el sector público. Puede parecer más fácil reunir una masa crítica de experiencia en seguridad digital a través de un organismo central, ya que el grueso de los retos técnicos de la seguridad digital es común a todos los sectores."

¿Cuál es el modelo colombiano? ¿Cuáles son sus pros y contras? ¿Cómo los potencian y mitigan? nada de eso se explica en el documento justificativo del decreto.

Uno puede deducir que Colombia apuesta por una gobernanza centralizada en una estructura con cinco organismos Comité Nacional de Seguridad Digital (queda a cargo de la política), la Coordinación Nacional de Seguridad Digital (es el que hace la coordinación sectorial), los Grupos de Trabajo de Seguridad Digital, las Mesas de Trabajo de Seguridad Digital y finalmente los Puestos de Mando Unificado de Seguridad Digital (los tres últimos son los encargados de operar la política).

Lo que vemos es que la evolución en el tiempo ha ampliado la participación intergubernamental, pero no ha disminuído su subordinación a la mirada de la seguridad nacional. La gobernanza en el decreto no es expresa sobre el rol del Ministerio de Defensa, que sin duda es protagonista. Reiteramos que entendemos su protagonismo, pero como ya explicamos, si estamos hablando de una política nacional la gobernanza precisamente el propósito es el de abordar la complejidad e ir más allá de la seguridad nacional.

La gobernanza que se diseña en el decreto es una que asume un escenario estático de qué protege y cómo lo protege. Es decir, ella misma no está diseñada para definir el qué se protege y está limitada frente a su relación con una de las partes interesadas, los operadores, que quedan bajo la supervisión del Ministerio de Defensa. Todas las críticas mencionadas sobre un diseño estático frente a una realidad dinámica aplican en este campo, así como lo limitado de tener una mirada de seguridad nacional.

El decreto propone un organismo que define la política al más alto nivel pero en un ente tan concurrido que hay que preguntarse cómo abordará los retos que suponen un modelo centralizado. Nada en el esquema de gobernanza propuesto habla de cómo articularse con las múltiples partes interesadas y mucho menos de lo que debería ser central en una política actualizada, cómo hará la gestión del riesgo digital nacional que es por supuesto el elefante en la sala.

Propuesta

Si la política nacional que estamos discutiendo es la del sector de seguridad nacional esta visión requiere ajustes -sobre todo en el terreno de controles y seguimiento a estas actividades- pero tiene sentido.

Si es la política nacional de seguridad digital, la prioridad de la gobernanza deberá ser la gestión nacional del riesgo digital, que determina qué se protege, cómo y cómo se articula con los otros actores interesados (privados y sociedad civil).

Como mínimo el mecanismo intergubernamental del decreto en todos los niveles (incluídos los operativos) debe tener espacios de participación y articulación con las múltiples partes interesadas.

2.6. La política nacional de gobernanza de seguridad necesita proteger a los investigadores de seguridad digital y requiere desarrollar una ruta de divulgación de vulnerabilidades

El trabajo temático más reciente dentro del grupo de seguridad digital de la OCDE ha sido precisamente la gestión de vulnerabilidades que incluye proteger a los investigadores de seguridad digital y la creación de una respuesta coordinada a sus reportes de vulnerabilidades. En 2021 la OCDE publicó varios documentos que buscan apoyar a los estados en el desarrollo de sus políticas nacionales. Esto fue totalmente ignorado en el decreto que estudiamos, incluso si sobre este tema los Conpes ya venían avanzando y el último tenía compromisos regulatorios en la materia.

El Conpes 3995 de 2020 estableció en cabeza del Ministerio de Defensa dos obligaciones relacionadas con la atención de vulnerabilidades cibernéticas: la primera, es estandarizar un mecanismo de reporte de incidentes y vulnerabilidades cibernéticas[30] que permita identificarlos, evaluarlos y comunicarlos a los interesados y, la segunda, es crear "un modelo para la divulgación periódica de vulnerabilidades en todos los sectores con un alcance definido entre los puntos de contacto de los propietarios y operadores de activos que soportan actividades críticas y las instancias pertinentes del Gobierno nacional".

A la fecha, pese a los esfuerzos de Fundación Karisma por establecer o participar de la formulación de la ruta de divulgación y atención de vulnerabilidades, no hemos logrado establecer con certeza cuál será la metodología o estructura de tales mecanismos. Siendo la única información certera que hemos recibido el *Marco contextual del modelo para la divulgación periódica de vulnerabilidades* hecho por MinDefensa para la definición de tal política y el plan de comunicación y divulgación de la ruta hecho por MinTIC. Documento que establecía el periodo de comentarios ciudadanos de la ruta de vulnerabilidades a finales del mes de diciembre, plazo que no fue cumplido.

Dicho esto, reiteramos que es preocupante que la política nacional de gobernanza digital no reconozca la importancia de los investigadores, incluya una ruta para la atención o divulgación segura de vulnerabilidades y se hable no solo de la importancia de esto en el entorno económico sino también en el social donde poblaciones como periodistas, defensores de derechos humanos o activistas son frecuentemente blanco de estos problemas.

En el decreto a pesar de que se definen las vulnerabilidades, lo que hace pensar que el decreto regulará el tema, en todo el desarrollo de la norma no se hacen más menciones al asunto.

Propuesta

Se debe reconocer la importancia de los investigadores y la obligación del estado en su protección. Las rutas de divulgación de vulnerabilidades facilitan a los gobiernos recibir información sobre sus vulnerabilidades de seguridad digital y coordinar una respuesta efectiva.

Por tal razón, es necesario que se cree una ruta coordinada para la divulgación y atención de vulnerabilidades. Para construir confianza múltiples partes interesadas económica y social de la seguridad digital, exigencia de la OCDE y del Conpes 3995 de 2020, potenciar el bienestar de las personas y el de las sociedades en su conjunto, así como garantizar una protección adecuada de los derechos de los ciudadanos es necesario implementar lo antes posible una ruta de divulgación de vulnerabilidades y mecanismos para atender dichas vulnerabilidades.

[30] Una vulnerabilidad digital es un error de diseño o de implementación, o una debilidad que tiene un equipo, programa, servicio o tecnología que puede ser explotada para comprometer la información o la seguridad de un sistema. Fuente: https://web.karisma.org.co/comunicado-de-prensa-nuevo-reporte-de-la-ocde-reconoce-el-trabajo-de-karisma-en-la-construccion-de-una-ruta-para-la-divulgacion-de-vulnerabilidades-en-colombia/